Business Software Alliance

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

November 23, 2026

Ms. Countryman:

The Business Software Alliance appreciates the opportunity to provide comments to the Securities and Exchange Commission ("SEC") in response to Chairman Atkins's request for comments on reforming Regulation S-K. We respectfully request the SEC strike Item 1.05, which contains the requirement that registrants report material cyber incidents within four days business days on Form 8-K, because requiring disclosure of a material cyber incident while response efforts remain underway will undermine those efforts and increase risks to registrants and their customers, other companies, and the public.

The Business Software Alliance (www.bsa.org) is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

Item 1.05 Material Cybersecurity Incidents, requires a registrant that determines it is the victim of a material cybersecurity to "describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations" within four days. It also contains limited, but insufficient exceptions.

The requirement's four-day disclosure timetable may force a registrant to announce an incident before the registrant has responded to or recovered from the incident. This timing would both amplify existing risks and create new ones, including by:

- Alerting attackers before systems are protected. Disclosure could reveal that a registrant has detected an intrusion while the attacker still has access, prompting the attacker to accelerate data theft, encryption, destruction, or disruption before defenders can prevent it.

200 Massachusetts Avenue, NW Suite 310 Washington, DC 20001
202.872.5500 **www.bsa.org**

- Encouraging additional attacks. Disclosure could attract other attackers to a registrant whose systems remain vulnerable or encourage exploitation of the same weakness at other companies.
- Disrupting investigations and coordinated responses. Disclosure could compromise efforts to share information with the government and other critical infrastructure organizations to help them protect their systems, and detect and respond to attacks, as well as efforts to identify attackers and dismantle malicious infrastructure.

Ultimately, in a threat environment that is increasingly risky due to nation-state actors and autonomous attacks, the requirement to disclose a material cyber incident within four days is making it harder for cyber defenders and riskier for all stakeholders.

To be clear, absent this requirement, registrants still have an obligation to disclose material information, whether it is related to cybersecurity or not, and this obligation will continue to ensure the SEC can achieve its mission to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."

For these reasons BSA recommends the SEC strike this requirement, which would additionally align with President Trump's Cyber Strategy for America, which calls for cybersecurity regulations "to ensure that the private sector has the agility necessary to keep pace with rapidly evolving threats." BSA appreciates the opportunity to provide input into the SEC's efforts and looks forward to working with the SEC to achieve our shared goal of a more secure and resilient digital ecosystem.

Sincerely,

Henry Young
Senior Director, Policy